A Proposal for the Future Governance of California's Information Technology Programs and Resources

By

J. Clark Kelso
Chief Information Officer
State of California
February 11, 2003

STATE CHIEF INFORMATION OFFICER
J. Clark Kelso (clark.kelso@opr.ca.gov)
1400 10th Street
Sacramento, CA 95814
(916) 739-7302 / (916) 739-7072 (fax)

February 11, 2003

Governor Gray Davis
State Capitol
Sacramento, California 95814

Dear Governor Davis:

By Executive Order D-57-02 (May 31, 2002), you directed me to "develop a proposal for the procurement, management and operation of the State's information technology systems."

On July 1, 2002, I submitted to you a preliminary report on "Information Technology Procurement, Management and Operations" where I described certain specific steps to be taken immediately to ensure appropriate oversight of ongoing information technology projects and to clarify roles and responsibilities over information technology projects and procurements in light of the Department of Information Technology's sunset on July 1, 2002. By Executive Order D-59-02 (July 1, 2002), you directed that those immediate measures be implemented. My preliminary report also included tentative recommendations for a permanent information technology governance structure.

After much further deliberation and consultation with leaders in state government and experts outside of state government, I am now ready to submit to you my final recommendation regarding the best governance model for California's information technology programs and resources. I look forward to receiving additional reaction to this final proposal from many interested stakeholders and to working with the Legislature to re-establish in statute an effective and efficient governance structure for California's information technology programs and resources.

J. Clark Kelso
Chief Information Officer
State of California

Table of Contents

I. Fundamentals of Information Technology Governance

A. The Mission of Information Technology

The governance structure proposed in the Information Technology Act of 2003 (the "Act" is reprinted below in the Appendix) supports the following mission for the use of information technology by state government:

> The State will manage, deploy, and develop its information technology resources to support responsive and cost-effective State operations and to establish timely and convenient delivery of State services, benefits, and information.

In California State government, information technology's primary role is to support and enhance State operations. Accordingly, the governance structure for managing the State's information technology program needs to be aligned with the governance structure for State operations. Otherwise, there will be a mismatch between the State's information technology program and the State operations and programs that information technology is designed to support.

Recognizing that State government in California is large, complex and decentralized, consisting of many independent constitutional officers and independent or partially independent organizational entities, fulfilling the mission will require a governance structure that facilitates coordination across organizational boundaries and builds upon and exploits the existing, well-established centers of authority (i.e., the state's major control agencies: Finance, General Services and Personnel Administration).

B. Principles of Information Technology Governance

The Act also draws upon the following fundamental principles of information technology governance:

1. Cost-effective information technology must be driven by an organization's business needs, and not by the technology itself, and should be procured using processes that ensure receipt of best value.

2. The State's Chief Information Officer should provide strong leadership, serving as the overall technology architect and strategic planner.

3. Statewide strategies and plans must be based upon broad input from a wide range of stakeholders and experts.

4. Technology strategic planning must be aligned with business strategies and have relevance for both current and anticipated needs.

5. There must be a strong connection between strategic planning and operational implementation.

6. There needs to be an identified, public forum for discussion, oversight and coordination of information technology activities.

7. Governance roles should be assigned based upon departmental core competencies.

8. There must be clearly assigned roles and responsibilities to ensure accountability.

9. A strong policy and procedural framework must be articulated and enforced.

10. All departments must be involved in enforcing compliance.

11. IT performance must continually be assessed and reported.

II. Governance Framework

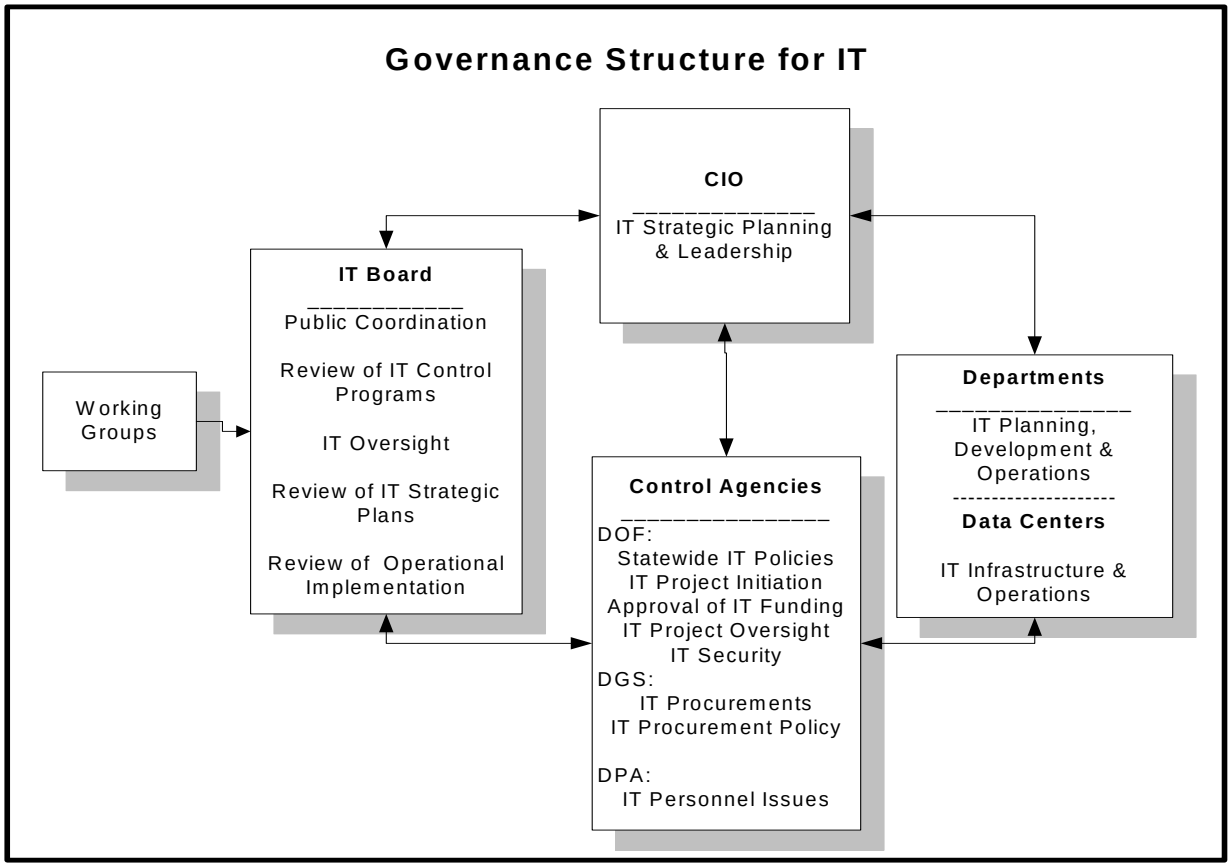
The Act establishes a governance framework to promote (1) successful and relevant strategic planning and decision-making, (2) oversight and alignment of information technology projects and operations to ensure consistency with strategic policies, (3) operational implementation by those most directly responsible for program performance, and (4) visible and open coordination, oversight and accountability. That framework assigns the following roles and responsibilities:

- State Chief Information Officer ("State CIO"): Strategic Planning and Leadership.

- Control Agencies (Finance, General Services, Personnel Administration): Statewide Policies, Procedures, Approvals and Oversight.

- Departments and Agencies: Operational Planning and Implementation.

- Information Technology Board: Coordination, Review of Strategic Plan(s), Review of Control Agency Programs, and Review of Operational Implementation.



A. The State Chief Information Officer

California needs a strong State CIO to provide leadership for the State's information technology program. A State CIO with a clear enterprise perspective can establish for the State a strategic vision for the coordinated planning, acquisition and development of cost-effective information technology solutions. The State CIO's role, then, is as a strategic planner and architect for the State's information technology program, and as a leader in formulating and advancing a vision for that program.

The Act establishes the State CIO in the Office of the Governor to provide vision and direction for the State's information technology investments through strategic planning. The State CIO will be appointed by the Governor subject to confirmation by the Senate.

1. Strategic Planner

Strategic planning is a disciplined, inclusive process which, if done properly, results in fundamental decisions to shape and guide an organization's near-term future (i.e., three to five years) in light of a changing environment and taking into account the organization's purpose, culture and resources.

The Act requires the State CIO to formulate and periodically update one or more strategic plans for the State's use of information technology. These plans would address foundational information technology issues for State government. The following list of topics suggests the type of issues that would be appropriate for consideration in a statewide strategic plan:

- Whether State government needs a coherent statewide information technology architecture for its information technology infrastructure, what such an architecture might consist of (e.g., standards to promote interoperability and development of statewide networks or applications) and how such an architecture should be developed;

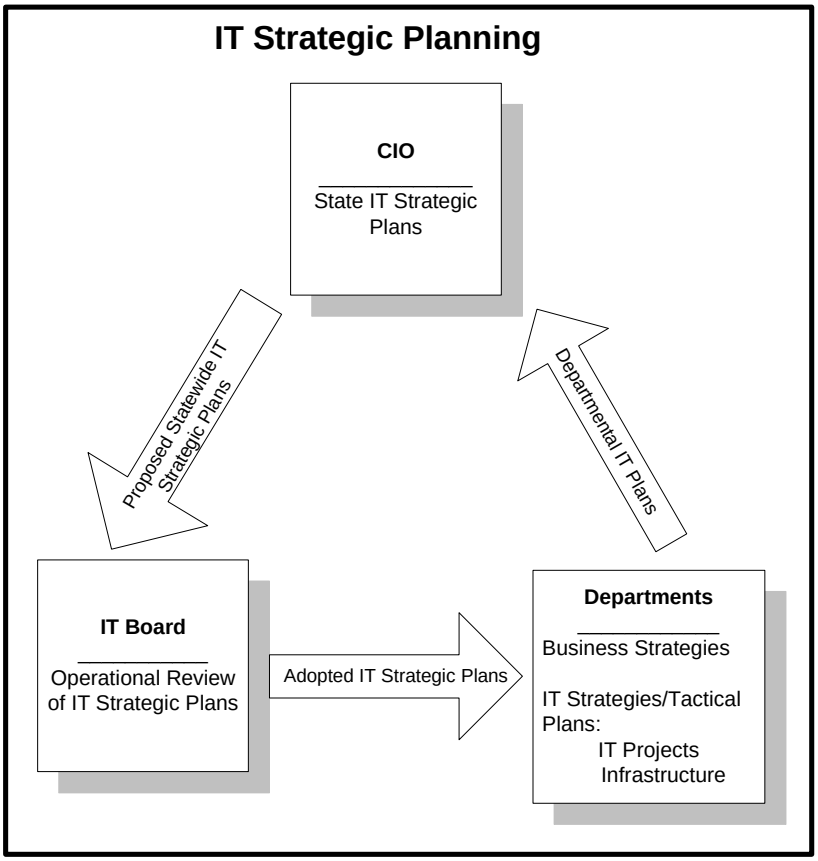
- How State government should organize and manage its presence on the Internet (i.e., e-Government);

- The extent to which computing resources should be aggregated in data centers and the proper use of data centers;

- Whether State government should develop statewide "back office" applications (e.g., financial, human resource and e-procurement systems) and, if so, a prioritization for developing and migrating to such applications;

- How State government can further improve and professionalize its information technology and procurement work forces.

The State CIO will gather substantial input from, among others, State departments and agencies on their business needs, planned projects and information technology infrastructure so that the strategic planning process is consistent with the State's existing operations and business plans. The State CIO will use these reports and plans, in part, to identify common business concerns that will form the business basis for information technology strategies. The CIO will also evaluate these departmental and agency reports to identify potential conflicts or omissions in planned information technology activities with respect to adopted strategic plans.



Strategic planning is a continuous process that requires substantial stakeholder involvement and input from a broad array of perspectives both internal and external to State government. In short, the process must be *inclusive*, and the Act thus anticipates that the State CIO will consult with IT leaders within government, such as the Agency Information Officers and data center directors, and with experts from the private sector, the technology community and academia, among other entities.

2. Leader and Change Agent

California's State CIO needs to be a leader and agent of change. The demands of information technology leadership in California are so great, that the State CIO needs to be empowered to devote the vast majority of his or her time to sharing an IT vision and providing leadership and strategic guidance. Other important information technology governance activities, such as the development of policies and procedures, project approval and funding, oversight and operational implementation, must be made the primary responsibility of other entities. The State CIO, through his or her membership on the Information Technology Board, will remain properly connected to these governance and operational activities, yet remain free to fulfill his or her primary responsibilities.

B. The Control Agencies

1. The Department of Finance

a. General Powers Over Statewide Information Technology

The Department of Finance, because of its role as the chief budget adviser to the Governor and its responsibilities over project initiation evaluation, funding, informational technology oversight and information technology security, is the primary control agency with respect to information technology issues. Its central role in all of these areas gives it a unique ability to ensure that operational implementation by departments and agencies is consistent with information technology strategic goals and objectives. It also has a unique ability, even without any additional legislation, to enforce compliance with information technology policies and procedures.

As a complement to its existing authorities, the Act specifically directs Finance to establish and maintain a framework of policies, procedures and requirements for the initiation, approval, management and oversight of information technology projects and for the security of information technology data and assets. Finance will also assess departmental and agency performance of project management, oversight and success, as well as the causes for project failure, and report those overall assessments to the Information Technology Board.

Finance's project approval, management, and oversight powers are substantial, including the following:

- Review of projects for compliance with statewide strategies, policies and procedures;

- Granting or withholding approval to initiate information technology projects;

- Requiring departments to provide information to Finance necessary for oversight evaluation (e.g., whether the project is within scope, cost and schedule, and the identification of project risks);

- Directing the Office of State Audits and Evaluations (a unit within Finance) to conduct project oversight reviews;

- Requiring remedial measures to put a project back on track (e.g., independent assessments of project activities, establishment of remediation plans, and additional project reporting);

- Imposing sanctions for nonperformance including, but not limited to, restriction of future project approvals for non-mandated projects pending demonstration of successful project implementation, and revocation or reduction of delegated authority;

- Recommending to the Information Technology Board the suspension, reinstatement or termination of a project;

- Reverting funds after a project is terminated; and,

- Determining which state department or agency will use which data center, and approve the methodology that the Teale Data Center uses for computing costs and billing rates.

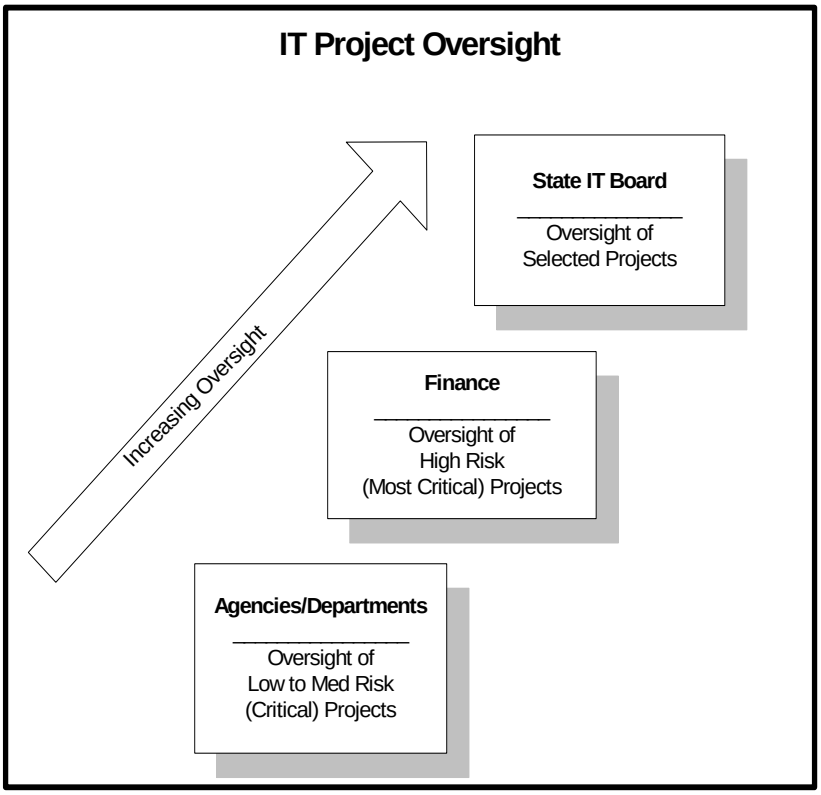
b. Finance's Initiation, Approval and Funding Program

Information technology project approval, funding, and support must be based on a full business case justification, acceptable risk and the department's capability to successfully execute the project. Finance develops and maintains the policies and procedures necessary to support the basic project approval, initiation and management requirements necessary for ensuring appropriate investments are being made in information technology.

c. Finance's Oversight Program

Finance defines oversight as an *independent* review and analysis of specific project activities and documentation to determine if an IT project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. Project oversight identifies and quantifies issues and risks affecting these project components.

Finance has established a framework for *graduated* oversight that will assess the risk, sensitivity and/or criticality of information technology projects, and assess the ability of the department or agency to effectively manage information technology projects and determine whether project oversight will occur at the department, Agency or Finance level.



d. Finance's Security Program

Finance is also responsible for leading the State's information technology security program. The State Chief Information Security Officer is located in the Department of Finance, leads its information technology security staff and is the State's primary representative to other public and private entities on statewide information security issues. Finance has the following responsibilities and powers with respect to information technology security:

- Development and maintenance of policies and procedures to provide for the security of the State's informational and physical assets, and for the preservation of the State's information processing capability, including policies for the confidentiality of security information;

- Coordination of research to identify solutions to problems affecting information security;

- Development and enforcement of policies and procedures to ensure that the technology supporting State business operations will continue to function in the event of a disaster;

- Review of security plans concerning the location and construction of information processing facilities for State agencies; and,

- Serving as the central contact point for notification of all security incidents involving unauthorized access, use or destruction of information technology resources.

2. The Department of General Services

The Department of General Services has general supervisory power over the State's procurement activities. Its statutes already give it the responsibility and authority it needs to be an effective control agency with respect to information technology. The Act therefore does not contain any additional statutory language with respect to General Services' authority over information technology procurements.

General Services is engaged in a substantial procurement reform effort, which began last year with the creation by Executive Order of the Governor's Task Force on Contracting and Procurement Review. The final report of that Task Force, delivered August 30, 2002, is available on the Department of Finance website at www.dof.ca.gov. General Services is actively implementing the recommendations of that Task Force and continuing discussions with Finance, the State CIO and others about additional steps to strengthen the State's information technology acquisition programs.

Department of General Services' approval of purchasing, management, and oversight powers are substantial, including the following:

- Conducting training to ensure agencies have training providing the knowledge and expertise to conduct information technology procurements, regardless of the vehicle used to procure (i.e., leveraged procurement or competitive procurement);

- Reviewing procurements and pre-procurement documents (i.e., the Information Technology Procurement Plan ("ITPP")) for compliance with statewide policies and procedures relative to procurement, and to ensure the ITPP adequately addresses procurement issues such as: (1) whether the procurement strategy is consistent with the contracting vehicle; (2) whether the project is ready for the procurement phase, the procurement vehicle is appropriate considering the project risk, contract management has been identified and the necessary knowledge and expertise is evident considering the project risk, and the contract management approach is adequate to ensure the contract is developed to achieve the program requirements and that project risk will be identified and mitigated; and, (3) whether recent legislation regarding conflict of interest and follow-on contracting (SB 1467 Bowen) is complied with.

- Assessing an agency's ability to purchase information technology goods and/or services based on staffing knowledge and expertise, and their ability to comply with state policies, procedures and guidelines;

- Delegating the responsibility for purchasing authority for information technology projects, on an agency basis;

- Requiring departments to provide information to DGS necessary for compliance evaluation (e.g., whether the procurement is within scope and follows developed guidelines, and identification of procurement risks);

- Requiring remedial measures to put a procurement back on track (e.g., independent assessments of procurement activities, establishment of remediation plans, and additional procurement reporting);

- Imposing sanctions for noncompliance including, but not limited to, revocation or reduction of delegated purchasing authority for future procurements, pending demonstration of successful training to conduct future procurements; and,

- Recommending to the Information Technology Board the suspension, reinstatement or termination of a procurement.

C. State Departments and Agencies

Information technology projects, infrastructure and resources are managed by the departments and agencies that have the day-to-day responsibility for State operations and services. This is the "front line" of the State's information technology program. It is appropriate that the departments with the greatest responsibility and accountability for state operations should also be responsible for the most focused planning, use and application of technology in support of those programs.

California's Agencies have a special role to play in the State's information technology governance structure. The Agencies have general planning, managerial and supervisorial responsibilities over the departments within their jurisdictions. This means that the Agencies and their Agency Information Officers ("AIOs") have important planning, management and oversight responsibilities. The State's CIO, Finance and General Services will continue to coordinate their activities with the AIOs.

D. The Information Technology Board

In light of the decentralized structure of California government, coordination and collaboration across organizational and constitutional boundaries is a strategic requirement. That coordination, and public accountability for the State's information technology activities, is the primary responsibility of the Information Technology Board.

The Information Technology Board consists of the Directors of Finance and General Services, the State CIO, and two members with expertise in information technology appointed by the State CIO (one of whom must be from a college or university). The Director of DPA will join the Board when personnel policy issues are presented for consideration.

The Board, administered primarily by the Department of Finance, will have the following responsibilities and powers:

- Review and adoption or rejection of the State CIO's strategic plans (but limiting its review to issues related to practical implementation of the plan leaving it to the CIO to resolve architectural and technological issues);

- Requiring departments and agencies to submit comprehensive plans addressing business needs, planned projects and information technology infrastructure;

- Periodic review of the project initiation, oversight and security programs at Finance and the IT procurement program at DGS;

- Conducting public IT project oversight hearings for selected projects, making findings and recommendations as a result of those hearings, and, as appropriate, suspending, reinstating or terminating a project with 30-day advance notification to the Legislature of any project that is terminated;

- For selected projects (e.g., large, complex integration projects that cross departmental boundaries or have statewide implications), require Board review and approval to continue after major project milestones;

- Establish working groups consisting exclusively of State employees to advise the Board on specific topics;

- Conduct hearings and make findings and recommendations on significant IT matters; and,

- Report a summary of the actions, findings and reports of the Board to the Legislature by August 31 annually.

It is anticipated that any significant developments in the State's information technology program will be brought to the Board for public vetting and, if appropriate, for action by the Board in the form of findings and recommendations. The Board should not become an obstacle to moving forward with the State's information technology program, and it would therefore be inappropriate to require Board approval for most information technology projects and acquisitions. However, there are great benefits in having major changes and any new, untested statewide initiatives brought before the Board for discussion and analysis.

Appendix

Information Technology Act of 2003

An act to add Chapter 5.5 of the Government Code (beginning with Section 11531), to add Chapter 3.5 of the Government Code (beginning with Section 13343), and to amend Sections 13400, 13401,13402, 13403, 13405, and 13406 of the Government Code, relating to information technology.

Chapter 5.5 Information Technology

Article 1. General

11531. Title

This chapter shall be known and may be cited as the Information Technology Act of 2003.

11532. Legislative intent and findings

(a) The Legislature finds and declares that information technology is an indispensable tool of modern government to support its operations and the provision of services, benefits and information to the public and business communities. To restore and maintain the public's trust in the state's management of its information technology investments, an open, responsive and accountable governance structure for information technology is required. The governance structure should, to the maximum extent possible, utilize existing resources in state government.

(b) The appropriate governance structure for the state is based on clear strategic thinking, sound management of existing information technology, and demonstrated accountability. The Legislature finds that:

(1) Cost-effective information technology investments must be driven first and foremost by the State's business and program needs, not by the technology itself. Strategic planning must be based on a sound understanding of both current and anticipated operational needs, as identified by the state's various departments, boards, and commissions.

(2) Statewide strategies must also be guided by broad input, drawing upon the knowledge, vision, and most effective practices of successful public, private and educational organizations.

(3) Strategic planning must be separate from but informed by day-to-day operational activities. To successfully maintain focus at the strategic level, the officer, as defined in Section 11533, should be the system architect and planner.

(4) For efficiency and effectiveness, the skills and expertise of existing state departments, agencies, and control agencies, should be the foundation for governing day-to-day information technology operations.

(5) To overcome any tendency for fragmented decision-making, the activities of the main providers of information technology governance must be coordinated.

(6) An effective bridge is needed between strategic planning and operational activities.

(7) There must be transparency and an opportunity for public input to strategic decision-making and major operational implementations.

(8) Governance roles and responsibilities must be clearly assigned.

(9) The policy and procedural framework for information technology management must be clear, consistent, updated and enforced.

(10) The responsibility for ensuring compliance with state policy and procedure, including the responsibility for competitive purchasing, must be embraced at each level of governance, with each level accountable for prompt, effective action.

(11) Information technology performance and progress, at both the project and department level, must be assessed and reported to ensure the effective management and control of information technology activities and the enforcement of state policies and procedures.

11533. Definitions

For purposes of this chapter, the following terms shall have the following meanings, unless expressly stated otherwise:

(a) "Officer" is the State Chief Information Officer.

(b) "Board" is the Information Technology Board.

(c) “Department” is the Department of Finance.

(d) “Strategic plan” is the documented result of a disciplined, inclusive process to make fundamental decisions to shape and guide the future of an organization, taking into account its organizational purpose, structure, culture, and resources, and the requirement of responsiveness to a changing organizational environment.

(e) “Information technology” includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, which may include voice, video, and data communications, requisite system controls, simulation, electronic commerce, and all related interactions between people and machines. This definition may be interpreted and further clarified by the Board pursuant to the authority in Section 11543(i).

(f) “Services” is contracted work for which payment is made to other than state employees. This includes, but is not limited to, consulting, technical staffing, professional staffing and temporary staffing.

(g) “Infrastructure” consists of information technology equipment, software, communications networks, facilities, and staff. Specifically included in statewide infrastructure are data centers and wide-area networks with their associated management and support capabilities.

(h) “Control agencies” are the Department of Finance, the Department of General Services and the Department of Personnel Administration.

11534. Governance framework

The purpose of this chapter is to provide a governance framework for information technology that is aligned with and responsive to the complex, decentralized structure of California government. A primary strategic objective for this framework, both in decision-making and operational implementation, is effective coordination across organizational boundaries.

The governance framework for information technology consists of the following elements to ensure successful planning, operations, and accountability:

(a) Strategic planning is provided by the State Chief Information Officer, created in Section 11535;

(b) Oversight and alignment of the state's information technology program and projects with the strategic plan is provided by the state's existing control agencies through information technology procedures and policies;

(c) The Information Technology Board, created in Section 11539, coordinates the information technology activities of the state's control agencies with each other and with the vision and direction provided by the State Chief Information Officer. The Board also provides a public forum for the highest level of information technology oversight.

(d) Operational implementation is the responsibility of state departments and agencies.

Article 2. Information Technology Strategic Planning

11535. State chief information officer

The State Chief Information Officer is hereby created in the Office of the Governor to provide vision and direction for the state's information technology investments through strategic planning. The officer shall be appointed by and responsible to the Governor and confirmed by the Senate.

11536. Responsibilities

The State Chief Information Officer shall advise the Governor on the strategic management and direction of the state's information technology resources. In this capacity, the officer shall:

(a) Engage in the formulation, evaluation, and updating of one or more strategic plans and the planning process for the state's use of information technology. The first strategic plan shall be submitted to the board no later than one year after the effective date of this act. Each plan, once adopted by the board, shall be reviewed annually by the officer for progress in meeting the plan's objectives and shall be revised by the officer and resubmitted to the board every three years.

(b) Work with and through the board to provide state departments and agencies with clear direction on the minimum requirements for the periodic reporting, to the officer, of business needs and planned projects and infrastructure for information technology to meet business needs and align with the state information technology strategies.

(c) Review reports received pursuant to (b) above and inform the board of significant deficiencies in reporting by state departments and agencies.

(d) Evaluate information provided in reports submitted pursuant to (b) above by state departments and agencies, as well as state information technology programs, identify potential conflicts or omissions in their planned information technology activities with respect to adopted statewide strategic plans, and recommend to the board new state policies, programs and actions, or amendments of existing programs, as required, to resolve conflicts, advance statewide information technology goals to respond to emerging business needs and opportunities, and to assure that state information technology policies

and programs conform to adopted strategic plans.

11537. Powers

The officer has the power to require state departments and agencies to submit reports to the officer on matters that will assist the officer in meeting the duties described in Section 11532(a). In exercising this power, it is the intent of the Legislature that the officer shall work through the administrative authority of the board to the extent practicable.

11538. Cooperation in developing strategic plans

(a) In developing a strategic plan for the state's use of information technology, the officer shall cooperate with the board in crafting a plan that translates readily from the strategic level to practical operations. Similarly, when the officer works with the board to establish or amend a planning process, the officer shall cooperate with the board in developing a process that is practical to implement. When the board advises the officer that an element of a strategic plan or a planning process needs modification to be implemented successfully, the officer shall review its planning requirements with the objective of resolving the board's concern.

(b) State departments and agencies shall cooperate with the officer by providing, on a timely basis, any required reports and clarification of any information submitted.

Article 3. Information Technology Coordination

11539. Information Technology Board

There is hereby created in state government the Information Technology Board. The Board consists of the State Chief Information Officer, the Director of Finance, the Director of General Services, and two members with expertise in information technology appointed by the State Chief Information Officer. One appointed member shall be employed by a college or university in California. For the purpose of reviewing workforce matters related to the state's information technology professional staff, the Director of Personnel Administration shall be a member of the board.

11540. Reimbursement for actual expenses

Members of the board shall receive no compensation for their services under this chapter, but shall be reimbursed for their reasonable expenses incurred in attending meetings and conducting the business of the board. Reimbursement of reasonable expenses for members employed by the State shall be the responsibility of each board member's employing department or appointing power. Reimbursement of reasonable expenses for any member not employed by the State shall be provided by the Department of Finance.

11541. Administration

The Director of Finance shall administer this part and provide assistance to the board, as it requires. The Director of General Services shall also provide assistance to the board, as it requires.

11542. Responsibilities

The board shall do all of the following:

(a) Review strategic plans and policy analyses submitted by the officer for adoption, advising the officer of issues affecting the ability to implement a plan.

(b) Upon request of the officer, direct a state department or agency to amend, update, or replace the report, received by the officer pursuant to Section 11536(b), to correct any significant deficiencies noted by the officer, and to establish the timeframe for resubmission to the officer. A state department or agency so directed may present arguments in support of its report to the board. Failure to comply with board direction may be cause for the board to invoke powers under Section 11543(h).

(c) Engage in systematic and periodic review of the state's information technology project initiation, oversight and security programs administered by the Department of Finance, the state's information technology procurement program administered by the Department of General Services, and any information technology program administered by any state agency selected by the board for examination.

(d) Establish criteria for review of information technology projects selected by the board. For projects the board does not select for project review, the board may delegate all powers in Section 11543 related to project review to the Department of Finance.

(e) Conduct information technology project oversight hearings, make findings and recommendations to state departments, agencies and control agencies, and exercise the powers provided in Section 11543, with respect to any project selected by the board for review or pursuant to policies or procedures adopted by the Departments of Finance or General Services;

(f) Conduct hearings and make findings and recommendations to state control agencies and the officer on various information technology matters, including enterprise-wide technology initiatives, processes, policies and procedures.

(g) Report a summary of the actions, findings and reports of the board to the Legislature by August 31 annually.

11543. Powers

The board may exercise the following powers:

(a) Adopt or reject a strategic plan submitted by the officer, providing that rejection must be based on issues related to practical implementation of the plan.

(b) Require additional information in the periodic reports, submitted by state departments to the officer pursuant to Section 11536(b) and as determined by the board, if the board finds that such information is needed for operational guidance, and if the officer concurs. The board may also impose reporting requirements, separate from those imposed by the officer, on state departments, agencies, and control agencies.

(c) Establish working groups from state employees, as needed, for issues and with membership determined at the board's discretion, to advise the board on any information technology matters.

(d) Pursuant to Section 11542(d), establish criteria by which information technology projects are selected for review by the board.

(e) Require state departments or agencies administering information technology projects selected for board review to provide all pertinent information on project performance, including but not limited to:

(1) the degree to which the project is within approved scope, cost and schedule;
(2) all project issues, risks and remediation efforts; and
(3) the estimated schedule and costs for project completion.

(f) Establish project findings and recommendations and direct departments and agencies on further reporting requirements.

(g) For any information technology project that has been approved by the Department of Finance pursuant to subsection (g) of Section 13345, that the board has selected to review, require the state department or agency administering the project to obtain the board's approval to initiate any phase, task, or step that is identified in the approved project schedule. Requests for approval to proceed shall be in accordance with processes and timeframes that the board shall establish or shall authorize its staff to establish, working in cooperation with state control agencies. The Board may delegate its power to approve initiation of any phase, task, or step that is identified in the approved project schedule, pursuant to this subsection, to the Department of Finance. The Department of Finance shall annually report to the Board actions taken under the authority delegated to the Department of Finance by the subsection. Nothing in this subsection shall be read to conflict with the responsibilities and authority of the Department pursuant to Sections 13344, 13345, and 13346. When necessary, the board and the Department shall work jointly to establish approval points throughout the project lifecycle.

(h) Suspend, reinstate, or terminate a project. The Board may delegate its power to suspend, reinstate, or terminate, pursuant to this subsection, to the Department of Finance. The Department of Finance shall annually report to the Board actions taken under the authority delegated to the Department of Finance by the subsection. Nothing in this subsection shall be read to conflict with the responsibilities and authority of the Department pursuant to Sections 13344, 13345, and 13346. The Department of Finance shall notify the Legislature of all project suspensions and reinstatements. The Department of Finance shall provide a 30-day advance notification to the Legislature of projects that are terminated. After notice has been provided to the Legislature, and pending the expiration of 30 days, the Board may require the state department or agency administering the project to stop expending funds on the project.

(i) Interpret and clarify the definitions set forth in Section 11533 (e) and (g). The Board may exercise this authority regarding Section 11533 (e) as it affects telecommunications only with the concurrence of the Department of General Services.

11544. Application of chapter

The provisions of this chapter shall not apply to the University of California, the California State University, the State Compensation Insurance Fund, the community college districts, agencies provided for by Article VI of the California Constitution, or the Legislature.

Chapter 3.5 Statewide Information Technology

13343. Definitions

The definitions in Section 11533 shall apply to this chapter.

13344. Responsibilities

The Department of Finance shall have the following responsibilities relating to information technology project approval, management and oversight programs:

(a) Establish and maintain a framework of policies, procedures and requirements for the initiation, approval, management and oversight of information technology projects. This includes responsibility for related sections in the State Administrative Manual.

(b) Possess and control all relevant records and papers held for the benefit and use of the former Department of Information Technology in the performance of its statutory duties, powers, purposes and responsibilities.

(c) Establish and maintain criteria for state departments and agencies to report information technology activities to the Department of Finance.

(d) Assess departments and agencies on their performance of project management, project oversight and project success. Annually report the overall assessment findings to the Information Technology Board.

13345. Authority

The Department of Finance may exercise the following powers relating to information technology project approval, management and oversight programs:

(a) Review proposed information technology projects for compliance with statewide strategies, policies and procedures.

(b) Require departments to provide information on information technology projects, including, but not limited to:

(1) the degree to which the project is within approved scope, cost and schedule;

(2) all project issues, risks and remediation efforts; and

(3) the estimated schedule and costs for project completion.

(c) Require departments to perform remedial measures to information technology projects to achieve compliance with approved project scope, cost and schedule, as well as statewide strategies, policies, and procedures. These remedial measures may include, but are not limited to:

(1) independent assessments of project activities funded by the administering department or agency;

(2) establishment of remediation plans;

(3) hiring vendors with project-required technical experience funded by the administering department or agency; and

(4) additional project reporting.

(d) Direct the Office of State Audits and Evaluations (OSAE) to conduct reviews of information technology projects to determine the degree to which they are within approved scope, costs and schedule, and the degree to which any required remediation activities have been successful. The cost of the review will be funded by the department or agency administering the project.

(e) Establish sanctions for nonperformance by departments and agencies, including but not limited to:

(1) restriction of future project approvals for non-mandated projects pending demonstration of successful project implementation; and

(2) revocation or reduction of delegated authority.

(f) Make recommendations to the Information Technology Board to suspend, reinstate, and terminate information technology projects.

(g) Grant or withhold approval to initiate information technology projects.

(h) Determine which state department or agency will use which data center, and approve the methodology that the Teale Data Center uses for computing costs and billing rates.

(i) Pursuant to Section 11543(h), revert unencumbered funds to the fund from which the appropriation was made, after a project is terminated.

13346. Security

The Department of Finance shall do all of the following relating to the State's information technology:

(a) Develop policies and procedures for the confidentiality of information.

(b) Develop policies and procedures necessary to provide for the security of the state's informational and physical assets and the preservation of the state's information processing capability.

(c) Coordinate research and identify solutions to problems affecting information security.

(d) Appoint a state information security officer who shall represent the state to the federal government, other agencies or state government, local government entities, and private industry on issues that have statewide impact on information security.

(e) Develop policies and procedures and review compliance therewith of departments, agencies and control agencies to ensure that the technology supporting state business operations will continue to function in the event of a disaster.

(f) Maintain the confidentiality of information about agency operational recovery plans. Such information shall not be disclosed to the public.

(g) Review and advise on security plans concerning the location and construction of information processing facilities for state agencies; keep confidential information about security plans, features, and vulnerabilities of planned and existing information processing facilities.

(h) Maintain the confidentiality of security and operational recovery information received pursuant to Section 13347.

(i) Investigate any security incident reported pursuant to Section 13347, as the Department deems necessary.

13347. Security incident notifications

(a) State agencies shall notify the Department of Finance, or its designee, of all incidents involving the intentional unauthorized access or unauthorized intentional damage to, theft of, or modification or destruction of, electronic information, and the damage to, or destruction or theft of, data processing equipment, or the intentional damage to, or destruction of, information processing facilities.

(b) Information about incidents described in (a) above received by the Department of Finance, or its designee, the disclosure of which poses a threat or potential threat to the safety or security of the personnel, property, buildings, facilities, technology infrastructure or equipment, including electronic data, owned, leased or controlled by the State, shall be considered confidential and shall not be disclosed to the public.

13348. Requirements for state department and agency information security officer

The chief executive officer of each state agency that uses, receives, or provides information technology services shall designate an information security officer who shall be responsible for implementing state policies and procedures regarding the confidentiality and security of information pertaining to his or her respective agency. The policies and procedures shall include, but are not limited to, strict controls to prevent unauthorized access to data maintained in computer files, program documentation, data processing systems, data files, and data processing equipment.

13349. Confidentiality requirements for vendors

Any contract entered into by any state agency that includes provisions for information technology security assessments, systems design, programming, documentation, conversion, equipment maintenance, and similar aspects of information technology services shall contain a provision requiring the contractor and all of his or her staff working under the contract to maintain all confidential information obtained as a result of the contract as confidential and to not divulge that information to any other person or entity.

13350. Application of chapter

The provisions of this chapter shall not apply to the University of California, the California State University, the State Compensation Insurance Fund, the community college districts, agencies provided for by Article VI of the California Constitution, or the Legislature.

Section 13400 of the Government Code is amended to read:

13400. This ~~act~~ *chapter* shall be known and may be cited as the Financial Integrity and State Manager's Accountability Act of 1983.

Section 13401 of the Government Code is amended to read:

13401. (a) The Legislature hereby finds that:

(1) Fraud and errors in state programs are more likely to occur from a lack of effective systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* in the state agencies.

(2) Effective systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* provide the basic foundation upon which a structure of public accountability must be built.

(3) Effective systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* are necessary to assure that state assets and funds are adequately safeguarded, as well as to produce reliable financial information for the agency.

(4) Systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* are necessarily dynamic and must be continuously evaluated and, where necessary, improved.

(5) Reports regarding the adequacy of the systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* of each state agency are necessary to enable the executive branch, the Legislature, and the public to evaluate the agency's performance of its public responsibilities and accountability.

(b) The Legislature declares it to be the policy of the ~~State of California~~ *state* that:

(1) Each state agency must maintain effective systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* as an integral part of its management practices.

(2) The systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* of each state agency shall be evaluated on an ongoing basis and, when detected, weaknesses must be promptly corrected.

(3) All levels of management of the state agencies must be involved in assessing and strengthening the systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* to minimize fraud, errors, abuse, and waste of government funds.

Section 13402 of the Government Code is amended to read:

13402. State agency heads are responsible for the establishment and maintenance of a system or systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* within their agencies. This responsibility includes documenting the system, communicating system requirements to employees, and assuring that the system is functioning as prescribed and is modified, as appropriate, for changes in conditions.

Section 13403 of the Government Code is amended to read:

13403. (a) ~~Internal~~ *Systems of internal* accounting ~~and~~ *controls,* administrative *controls, and information security* controls are the methods through which reasonable assurances can be given that measures adopted by state agency heads to safeguard assets, check the accuracy and reliability of accounting *and other* data, promote operational efficiency, and encourage adherence to prescribed managerial policies are being followed. The elements of a satisfactory system of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, or information security controls,* shall include, but are not limited to, the following:

(1) A plan of organization that provides segregation of duties appropriate for proper safeguarding of state agency assets.

(2) A plan that limits access to state agency assets to authorized personnel who require these assets in the performance of their assigned duties.

(3) A system of authorization and recordkeeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

(4) An established system of practices to be followed in *the* performance of duties and functions in each of the state agencies.

(5) Personnel of a quality commensurate with their responsibilities.

(6) An effective system of internal review.

(7) Information security risk management policies, procedures, and practices that ensure the reliability of information systems and the protection of information assets.

(b) State agency heads shall follow these standards of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* in carrying out the requirements of Section 13402.

Section 13405 of the Government Code is amended to read:

13405. (a) To ensure that the requirements of this ~~section~~ *chapter* are fully complied with, the head of each agency ~~which~~ *that* the director determines is covered by this ~~section~~ *chapter* shall prepare and submit a report on the adequacy of the agency's systems of internal accounting *controls* and administrative ~~control~~ *controls* by December 31, ~~1983, and by December 31 following the end of each odd-numbered fiscal year thereafter~~ *2005, and every two years thereafter*.

(b) The report, including the state agency's response to report recommendations, shall be signed by the head of the agency and addressed to the agency secretary, or the director ~~of finance~~ for agencies without an agency secretary. Copies of the reports shall be forwarded to the ~~Legislature~~ *chair of the Joint Legislative Audit Committee*, the *State* Auditor ~~General~~, the Governor, and the ~~Director of Finance~~ *director*. Copies of these reports shall also be forwarded to the State Library where they shall be available for public inspection.

~~(c) By January 1, 1983, the director, in consultation with the Auditor General and the Controller, shall establish a system of reporting and a general framework to guide the agencies in performing evaluations on their systems of internal accounting and administrative control. The director, in consultation with the Auditor General and the Controller, may modify the format for the report or the framework for conducting the evaluations from time to time as deemed necessary.~~

~~(d)~~

(c) Any material inadequacy or material weakness in an agency's systems of internal accounting ~~and~~ *controls and* administrative ~~control which~~ *controls that* prevents the head of the agency from stating that the agency's systems of internal accounting ~~and~~ *controls and* administrative ~~control~~ *controls* provided reasonable assurances that each of the objectives specified above was achieved, shall be identified and the plans and schedule for correcting any ~~such~~ inadequacy described in detail.

(d) To ensure that the requirements of this chapter are fully complied with, the head of each agency that the director determines is covered by this chapter shall prepare and submit a report to the director on the adequacy of the agency's system of information security controls by December 31, 2004, and every odd numbered year thereafter. Any material inadequacy or material weakness in an agency's system of information security controls that prevents the head of the agency from stating that the agency's system of information security controls provided reasonable assurances that each of the objectives specified above was achieved, shall be identified and the plans and schedule for correcting any inadequacy described in detail. The confidentiality of the information

submitted to the director pursuant to this subsection shall be maintained and the information shall not be disclosed to the public.

Section 13406 of the Government Code is amended to read:

13406. (a) The head of the internal audit staff of a state agency or a division, as specified by the director, or, ~~in the event~~ *if* there is no internal audit function, a professional accountant, if available on the staff, designated as the internal control person by the head of the state agency or a division, shall receive and investigate any allegation that an employee of the agency provided false or misleading information in connection with the evaluation of the agency's systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls* or in connection with the preparation of the ~~annual~~ *biennial* report on the systems of internal accounting ~~and~~ *controls,* administrative ~~control~~ *controls, and information security controls*.

(b) If, in connection with any investigation under subdivision (a), the head of the internal audit staff or the designated internal control person determines that there is reasonable cause to believe that false or misleading information was provided, he or she shall report in writing that determination to the head of the agency or the division.

(c) The head of the agency or division shall review any matter referred to him *or her* under subdivision (b), shall take ~~such~~ *any* disciplinary or corrective action as *that* he *or she* deems necessary, and shall forward a copy of the report, indicating therein the action taken, to the director within 90 days of the date of the report.